NETWORK AND DATA POLICY CONSIDERATIONS FOR EFFECTIVE NETWORK CENTRIC OPERATIONS

J. Katharine Burton
Institute for Defense Analyses
Alexandria, VA
(703) 885-6617
kburton@ida.org

Martin R. Stytz, Ph.D.
Institute for Defense Analyses
Alexandria, VA
(407) 497-4407
(703) 338-2997
mstytz@ida.org , mstytz@att.net

Gregory N. Larsen, Ph.D.
Institute for Defense Analyses
Alexandria, VA
(703) 845-6661
glarsen@ida.org

ABSTRACT

The US military is undertaking an unprecedented transformation as a result of its adoption of a network centric operational philosophy. This transformation maximizes the military's reliance upon data superiority and decision superiority, but we have yet to develop the doctrine, systems, and data insights needed to fully exploit the physical capabilities for communication being developed. To redress the problem of translating human formulated policies into machine-actionable policies that maximize the use of network and computational resources, we must understand how to translate doctrine and policy into network and computational management policies. These network and computational management policies address implementation of network-centric operational needs and, these network and computational management policies are the only mechanisms available to commanders for insuring that the right data reaches the right user at the right time. The research that we report addresses the policy issues highlighted above and is intended begin the process of uncovering the requirements for network and data policy, exploring the effects of decision-making data demands on network and data policies, and examining the effect of network and data policy on the efficiency of network-enabled operations.

1. Introduction*

The US military is undertaking an unprecedented transformation as a result of its adoption of a network centric operational philosophy[1-7, 9, 10]. This transformation maximizes the military's reliance upon data superiority coupled with decision superiority to achieve overwhelming battlespace dominance. Because of this transformation, networks and the data they carry are now, more than ever before, viewed as force multipliers and critical assets. As a result, there has been a corresponding emphasis on research devoted to addressing the implications of adopting a network centric operations orientation as it relates to policy, military doctrine, computational power, and aggregate bandwidth/communications requirements. As a result of this research and commercial developments, there has been a corresponding increase in bandwidth available for operational needs and policy/doctrinal developments that illuminate techniques for best employing network and computational power to achieve decision superiority. And yet, the improvements in bandwidth, computational power, policy, doctrine and tactics do not correlate with a commensurate, corresponding increase in operational effectiveness. In short, our investments in physical capabilities and understanding of the network centric environment have not been as effective as would be reasonably expected. The reason for this unacceptable ineffectiveness is that we do not know how to knit together advances in physical capabilities (bandwidth and computational power) with advances in network centric policies and doctrine to achieve a dynamic, flexible, dominant network-centric force.

To redress the problem of translating human formulated policies into machine-actionable policies that maximize the use of network and computational resources, we must understand how to translate doctrine and policy into network and computational management policies. To achieve this goal, we must learn how to automatically translate intellectual decisions concerning policy into their physical manifestations as reflected in

* The views expressed in this article are those of the authors and do not reflect the official policy or position of the Department of Defense or the US Government.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Network and Data Policy Considerations for Effective Network Centric Operations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Institute for Defense Analyses,4850 Mark Center Drive,Alexandria ,VA,22311**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**23**	

network bandwidth allocations and other network/computational policies. Therefore, control and management of network resources[1] and the data that move across them are two crucial topics that we must address if we are to gain maximum operational advantage from other investments made in achieving network centric operational capabilities. Unfortunately, these two topics as well as the technological issues related to automatically translating command-level policy into network and data management policy are topics that, to date, have received relatively little consideration. Our goal is to examine these issues and provide insight into the decision space that must be mastered. In this paper we examine the spectrum of network and data policies and the policy translation/transformation issues that must be addressed to achieve an efficient network centric operational environment and the corresponding influence of these policies on efficient network-centric operations.

As will be discussed later in the paper, network and data control and management policy issues are of critical importance to the success of network centric operations for two reasons. First, these two classes of policies address implementation of network-centric operational needs and second, these policies are the only mechanisms available to commanders for insuring that the right data reaches the right user at the right time. Since network centric operations rely upon data and decision superiority coupled with rapid resource re-allocation to achieve decisive battlespace dominance, the network and data control and management policies must be established across the network in light of the needs and capabilities of the individuals who rely upon the network and its data. The network and data policies that are employed must support all user needs and requirements while also insuring that individual data needs for decision-making, the available bandwidth, the communication alternatives, the various mission priorities, and individual data security needs are all considered. As discussed in the paper, the network and data policies satisfy the users' requirements by allocating bandwidth to users, by allocating bandwidth to policy propagation uses, by allocating bandwidth for the transmission of assessments of user data needs, and by allocating different priorities to the different types of data as it moves between users. Because changes in network and data control and management policy must be made rapidly, tools that accurately translate the command-level policy decisions into network and data control and management policies are needed.

The network and data policy requirements are driven by five factors, 1) the mission for each organization on the network, 2) the current state of the battlespace, 3) the available communication channels within the network, 4) the data needs for each of the users' and commanders', and 5) security demands for each user and commander. These factors combine to define the data volume and latency needs for each user, thereby specifying the instantaneous bandwidth requirements for each user as well as the network security requirements. The five factors also define the instantaneous data veracity/truthfulness and data verification requirements for each user. Note that the network and data policy choices are complicated by the fact that the policies will be different for each user and unit, that circumstances will alter user and unit needs for data (thereby forcing dynamic policies), and policy as it relates to each user and each unit must change rapidly in order to effectively address their needs. The variety of demands placed upon network and data services coupled with the need for rapid change in network and data policies point to the need for intelligent agent assistance and human behavior models for each user to aid in network and data policy development. Therefore, intelligent agent assistance and human behavior models are essential to the process of translation of command-level policy decisions into network and data control and management policies. The need for intelligent assistants and human behavior models has been suggested by others as a response to the complexity and variety of the data available to each user in a network centric environment but the need for intelligent assistants and human behavior models is increased by the necessity for rapidly adapting network and data policies to changes in the five factors in order to effectively manage the network environment. Our research is intended to address the factors highlighted above and to uncover the requirements for network and data policy, to explore the effects of decision-making data demands on network and data policies, and to examine the effect of network and data policy on the efficiency of network-enabled operations. Our research is also intended to address the requirements for tools needed to knit together current and coming capabilities that are relevant to network centric operations into an effective network centric operational force.

The paper is organized as follows. Section Two holds a brief discussion of previous research related to the issues we address. Section Three presents a discussion of the requirements for network and data policy in a NCOE. Section Four contains a discussion of the range of network and data policies that can address the requirements and the types of translation tools required to knit the policies into a cohesive, responsive, effective

[1] The difficulties encountered in control and management of resources is a topic receiving more attention of late; see, for example, "An AI Planning-based Tool for Scheduling Satellite Nominal Operations," by Moreno, Borrajo, and Meziat, *AI Magazine*, vol. 25, no. 4, Winter, pp. 9-27.

force. Section Five contains a summary of our research to date and suggestions for further research in this field.

2. Background

"Train the way you will fight" is the policy for United States' military training and this philosophy has served the warfighter well as evidenced by the many successful operations executed around the world over the last decade. However, the US military is in the midst of a change in its philosophy, approach, and technologies used for warfare as we move toward small formations, small but extremely accurate weapons, and high speed movement all augmented by rapid, automated movement of data between and among all military components from the battlefield back to the logistics depot. This new form of warfare, in which a great premium is placed upon timely, accurate data, is called network centric warfare (NCW) [1-7, 9, 10]. For this future vision of warfare to be achieved and be effective there are a number of issues that must be addressed and solved in the real-world and in the world of simulation. In the NCW battlespace of the future, the coming capabilities in networks and computing portend a time when warfighters will become very dependent upon the unprecedented level of detailed data available concerning the situation within a battlespace. This reliance will induce foes to attempt to disrupt the data flows in an attempt to gain an advantage or to disrupt friendly operations. The interplay between friendly efforts to maintain their data operations and enemy attempts to disrupt them will inevitably result in conflict in the cyberworld, or cyberbattlespace.

Network-centric operations are military activities that are enabled and enhanced in effectiveness by the networking of the force. The ability to operate in a network-centric manner provides warfighters with a new type of data advantage, an advantage broadly characterized by significantly improved capabilities for sharing and accessing data. Network-centric warfare enables networked warfighters to leverage their data advantage to increase their effectiveness across a broad spectrum of mission areas. The key to this increase in effectiveness is data superiority. Data superiority is a state in the data domain wherein one adversary is able to establish a superior data position as regards other adversaries. Data superiority is enabled by an imbalance in the data domain but this imbalance can only be fully exploited by a network-centric force.

A network-centric force is effectively linked or networked by its network capacity and data infrastructure. A network-centric force has the capability to share and exchange data among the distributed elements of the force and has access to data whenever and wherever it is needed. However, current policies for data sharing and network operations inhibit achievement of this goal. In the next section, we will consider the requirements for a network-centric force and then turn to a discussion of how policy should change to satisfy these requirements.

3. Network and Data Policy Requirements

As is clear from the material presented in the preceding section, the ability of a network-centric force to operate effectively is correlated with the ability of data to move through the organization effectively and efficiently. However, while this statement is accurate it does not provide enough guidance to effectively assess the quality of the data flow and to identify areas within the organization where changes in policy and data flow processes can have the most effect. To help provide the guidance, we turn to a formal statement of our objectives for data movement within an organization.

Within a network centric organization, there are two sets of entities, sources of data and recipients of data. Let *r* be the set of data recipient entities and allow them to be arbitrarily labeled from 1 to n. Let *s* be the set of data source entities and allow them to be arbitrarily labeled from 1 to m. Let I_r be the data required by/destined for a particular recipient of data and *n* be the number of data recipients and let I_s be the data send from any source of data and *m* be the number of data sources. Then, $I_{r_a} \leftarrow I_{s_b}$ defines the instantaneous data volume (in bytes) between any source and recipient of data. We can then define $\mathbf{I_1}$ as:

$$\mathbf{I_1} = \left(\prod_{i=1}^{n} I_{r_i} \leftarrow \prod_{j=1}^{m} I_{s_j} \right) \qquad \textbf{(1)}$$

Therefore, I_1 is the total instantaneous volume of data moving from all sources of data to all recipients of data within an organization at any given time. Note that this definition is source-recipient topology neutral, technology neutral, and bandwidth independent. This definition also accounts for data moving on the network for both operational and network management purposes. Based this definition for $\mathbf{I_1}$, it is clear that for a network-centric force to be effective, its data capacity must not only be able to accommodate peak demands for transmission of operational data but also peak demands for transmission of operational data in conjunction with simultaneous peak demand for transmission of network management data. Clearly, $\mathbf{I_1}$ is always less than or equal to the maximum data volume demand imposed by an organization during an operation. In addition, the data transmission capacity for an organization must be greater than $\mathbf{I_1}$ if an

organization is to be network-centric. Using $\mathbf{I_1}$, we define data velocity $\boldsymbol{\varpi}$ within an organization at a given time $\boldsymbol{\tau}$ within an organization as:

$$\boldsymbol{\varpi}_{\tau} = (\mathbf{I_{1_{\tau}}} - \mathbf{I_{1_{\tau-1}}}) / \mathbf{I_{1_{\tau-1}}} \qquad (2)$$

For a network centric organization to operate at maximum effectiveness, data velocity must be able to change by a large amount in a very short period of time, which means that the data carrying capacity for the network is very responsive to rapid changes in load imposed by operational data as well as for network management data. Let $\mathbf{I_2}$ be the average time required for data to move from all sources to all recipients within an organization at any given time period $\boldsymbol{\tau}$ and let it be defined as:

$$\mathbf{I_{2_{\tau}}} = \left(\left(\prod_{i=1}^{n} I_{r_i} \leftarrow \prod_{j=1}^{m} I_{s_j} \right) \right) \div \sum \left(\Delta t \left(r_i \leftarrow s_j \right) \ \forall \ \left(r_i \leftarrow s_j \right) \neq 0 \right) \qquad (3)$$

Clearly, for a network-centric organization to be effective, $\mathbf{I_{2_{\tau}}}$ must be minimized at all times. In order to minimize $\mathbf{I_{2_{\tau}}}$, clearly there must be no contention for bandwidth within the organization and operational and network management data must be transmitted with equal promptness. Let $\mathbf{I_3}$ be the average time for priority data to move from all sources to all recipients of data of that given priority at any given time $\boldsymbol{\tau}$ within an organization. Let p_y be defined as the set y of priority data at that same time, and let $p_{y,\ y=1,x}$ be defined as the set of all priorities for data within an organization. Then $\mathbf{I_{3_p}}$ for a given message priority $\boldsymbol{y}$ at a time $\boldsymbol{\tau}$ is defined as shown in equation 4. And with this specification in hand, we can then define $\mathbf{I_3}$ for all message priorities within an organization at a given time $\boldsymbol{\tau}$ as shown in equation 5.

$$\mathbf{I_{3_{p_y}}} = \left(\left(\prod_{i=1}^{n} I_{r_i} \leftarrow \prod_{j=1}^{m} I_{s_j} \right) \right) \div \sum \left(\Delta t \left(r_i \leftarrow s_j \right) \ni \left(\left(r_i \leftarrow s_i \right) \neq 0 \ \wedge \ \left(r_i \leftarrow s_j \right) \subset p_y \right) \right) \qquad (4)$$

$$\mathbf{I_3} = \sum_{y=1}^{x} \mathrm{I}_{3_{p_y}} \div \mathrm{x} \qquad (5)$$

$$\mathbf{I_{4_r}} = \sum_{j=1}^{m} \left(t a_r - t n_r \right) \ \forall \ \left(I_r \leftarrow \prod_{j=1}^{m} I_{s_j} \ \ni \ \left(r_r \leftarrow s_j \right) \neq 0 \right) \qquad (6)$$

Let $\mathbf{I_{4_r}}$ be the time differential between the time when data is needed, $\boldsymbol{t_n}$,by a recipient and when it received, $\boldsymbol{t_a}$, by the recipient for a given time period. Then $\mathbf{I_{4_r}}$ for a given recipient $\boldsymbol{r}$ during that time period is defined as shown in equation 6: And $\mathbf{I_4}$ for an organization within that same time period is defined as:

$$\mathbf{I_4} = \sum_{r=1}^{n} \mathrm{I}_{4_r} \qquad (7)$$

Clearly, $\mathbf{I_4}$ for an organization should be minimized in order to improve network-centric effectiveness. In addition, it is clear that for a given recipient to receive the data of most importance to the recipient, $\mathbf{I_3}$ for the highest priority data for the recipient must be minimized in order to minimize $\mathbf{I_4}$ for the recipient. The efficiency of the

movement of data for a given data recipient **r,** called ψ, at time τ can then be defined as:

$$\psi_{r_\tau} = (l_{4_{r_\tau}} - l_{4_{r_{\tau-1}}}) / l_{4_{r_{\tau-1}}} \quad \textbf{(8)}$$

We define l_{5_r} as the time differential between the time when data is needed, t_n,by a recipient and when it received, t_r, by a data recipient for a given time period for data of a given priority y. l_{5_r} in a given time period is defined as: shown in equation 9:

$$l_{5_r} = \sum_{j=1}^{m} \left(ta_r - tn_r \right) \forall\ I_r \leftarrow \prod_{j=1}^{m} I_{s_j}\ \ni \left(\left(\left(r_r \leftarrow s_j \right) \neq 0 \right) \wedge \left(\left(r_i \leftarrow s_j \right) \subset p_y \right) \right) \quad \textbf{(9)}$$

l_{5_r} should approach zero for data of the highest importance for each recipient during any time period. Therefore, policies should be established such that priority data has a better chance of reaching a recipient when it is needed, and hence forcing l_{5_r} toward zero.

With these definitions in hand, let us turn to l_2 and examine it in more detail. For l_2, the differential for a given recipient **r** is composed of the sum of the time the data is spent in a transmission medium, **m**, the time spent in computing devices, **c**, the time spent in sensing systems, **s**, the time spent in releasability decision making, **rdm**, and the time spent in human analysis, **h**, or

$$l_{2_{r_t}} = \sum t_{r_m} + t_{r_c} + t_{r_s} + t_{r_{rdm}} + t_{r_h} \quad \textbf{(10)}$$

Clearly, t_{r_m}, t_{r_c}, **and** t_{r_s} are approximately constant for any given operation and change slowly in relation to a given operation or in relation to the rate at which new technologies can be widely deployed. Therefore, $l_{2_{r_t}}$ is controlled by t_{r_h} and $t_{r_{rdm}}$, which implies that policies should be established with the need to minimize the amount of time that data spends in human analysis and the amount of time that data spends in a releasibility decision. This same situation appears to hold for l_3, l_4, and l_5. This conclusion agrees with our intuition in that reductions in the time spent in human decision-making concerning releasilibility of data will improve the performance of the system when transporting important data to a recipient that needs the data. However, it is unclear whether improving the performance of the system in one of its components in regard to these parameters will insure an overall improvement in performance; additional research in the system engineering and composition aspects of data transport mechanisms in regard to network centric warfare is required.

Another approach to improving system performance that has been suggested is the use of intelligent agents. If intelligent agents are to be used to improve the data flow within an organization, the first priority for their use is for making decisions for releasibility since time saved making this decision pays the biggest dividend for improved performance of the network centric organization, for data movement within the organization, and to achieve the ultimate goal, which is to improve timely decision making. Of course, the user should not be overwhelmed with information[8], so the intelligent agents not only have to insure that the prioritized information reaches the user but also that the user is not inundated with information. Before moving on to a discussion of the data and network policies suggested by the work presented in this section, Table 1 summarizes the major metrics/variables defined in this section and a short specification for each.

Table 1: Major Metrics/Variables and Their Definitions

Metric/Variable	Definition
I_1	The volume of data moving from all sources of data to all recipients of data within an organization at any given time
I_2	The average time for data to move from all sources to all recipients within a time period
I_3	The average elapsed time for priority data of a given priority to move from all sources to all recipients of data of that priority at any given time.
I_4	The time differential between the time when data is needed by a recipient and when it is received.
I_5	The time differential between the time when data is needed by a recipient and when it received by the data recipient for a given time period for data of a given priority.
ϖ_τ	Data velocity within an organization at a time τ
ψ	The efficiency of the movement of data.

4. Policies and Tools

In the preceding section, we defined measures for data movement within an organization; measures that allow us to assess the efficiency of data flow, its velocity, the total data flow at any time, and measures to assess the ability of an data system to respond to the demands placed upon it during the course of an operation. In addition, we defined the metrics so that the data required to compute the figures of merit can be gathered. Nevertheless, while we have defined these metrics so that they can be applied to any combination of network configurations, it should be clear that we currently do not have the tools available to readily gather the required data, that we lack insight into the many factors that affect the metrics, and we lack the engineering tools required to design networks with the capabilities required to optimize the measures. Nevertheless, we do have some insights into the general qualities that the data transportation system should possess. The system should be able to deal with rapid changes in data transportation requirements and allow data to reach its recipients rapidly. Therefore, data and network policies should be constructed so that prioritized data receives preferential handling and so that the data spends little or no time in the $t_{r_{rdm}}$ state.

One clearly important parameter within a network centric organization is I_1. The data transportation system must be able to satisfy any demands placed upon it for data, and all things being equal, a system with a larger I_1 is better than one with a smaller I_1. One interesting question to be addressed is whether a system with a large I_1 but with a large overall ϖ_τ is better or worse than a system with a relatively smaller I_1 but also with a relatively smaller ϖ_τ. Additionally, the data transportation system must have a small value for ϖ_τ under all circumstances, because this will insure that not only can the system handle the data load and that it can also respond to changes in demand rapidly. Clearly, some of the values we have defined, such as I_3, I_4, and I_5 can not be affected to a large degree once an organization starts an activity, and so the organization should begin any activity with the capabilities in its data transportation system needed to minimize these values. However, it is clear that I_5 is an important parameter throughout the force and minimization of this value is an important goal and needs to be pursued via technology and via alteration of policies. Especially important are modification of policies controlling sensitive but important data, the need for attaining a small value for I_5 should be a major consideration when considering any policy related to data movement throughout a force. In order to insure that these values are minimized and because we can affect them only to a small extent once activity begins, simulations of network-centric activities where the appropriate data are gathered and analyzed are necessary. Clearly, the simulations should address as many possible environments as possible so as to insure that the data transport system can satisfy the demands placed upon it. The simulations should, therefore, possess as much fidelity as possible and the situations simulated should be repeated a sufficient number of times to insure statistical significance for the results.

5. Summary and Further Work

As noted above, the US military is undertaking an unprecedented transformation in its adoption of a network centric operational philosophy. This transformation increases to an unprecedented degree the military's reliance upon data superiority and decision superiority, but we have yet to develop the insights

needed to fully exploit the physical capabilities for communication being developed. To redress the problem of translating human formulated policies into machine-actionable policies that maximize the use of network and computational resources, we must understand how to translate doctrine and policy into network and computational management policies. This paper is a step in that direction.

The network centric paradigm for warfare in the future spans the entire spectrum of conflict. Given the breadth of the challenge, a number of issues arise that must be addressed in order to assure accurate data operations within a network centric warfare environment. For example, when performing military planning and operations in a network centric warfare environment, the operation and use of computer networks and software will increase in importance. This increasing reliance points to a need for training of operators that use the network so that they can gain the maximum advantage from the available data and also be able to recognize when the data is incorrect and/or the network and software are not functioning properly. In this paper, we have also raised the issue of preparing the network for its task, so in addition to preparing operators for network centric operations, simulation can prepare the network to address the demands that will be placed upon it during operational use.

One important area for future work is to extend the representations presented here. They should be extended in the degree of detail they capture and serve as the basis for developing further measures. In addition, the representations developed here should be extended so that network topologies, bandwidth availability, network attack, and other factors that affect performance in the real world are captured. However, additional work is also indicated.

Because of the attractiveness of the network and data for attack by an adversary, it is also apparent that data and network policies must be developed so that data moves from source to recipient in spite of attack and that priority traffic reaches its destination so as to minimize l_{4_r} for each recipient. It is apparent that for NCW to be successful as an operational paradigm into the future, the people and policies within the NCW battlespace must be prepared to deal with attacks upon the data resources that make NCW a viable strategy. In light of this need, operators and data technology specialists must be trained to be able to recognize and counteract a cyber attack against NCW data resources, which is not an easy task. This training and simulation activities are important future work that should be started as soon as practicable.

Another important area of research that must be addressed is the instrumentation of the network in order to acquire the data needed to compute the measurements that we have suggested in this paper. To properly instrument the network, need to determine where to place the sensors and the data they should gather. In addition, we must determine how to communicate performance data to a network operations center so that this communication has minimal impact upon the transmission of operational data, maintains efficiency for data transmission, and enhances the responsiveness of the network to changes in load and demand. To achieve these objectives, we believe that research is needed to determine the type(s) of sensors that are needed, the different means that can be employed to gather the data for the measurements, and research to assess which approaches to performance data acquisition and dissemination are the most useful and efficient.

A further area of research that is suggested is refinement of our knowledge about systems engineering and composition when assembling advanced systems of systems to support network centric warfare. We are currently woefully ignorant concerning the factors that influence overall system performance, the key interfaces between systems, the components of the system that most influence policy, the proper placement and priority for development of intelligent aids for routing and releasing data, or even how to recognize and adapt to changes in priority of data by various data recipients. In sum, we need to improve our knowledge about the theory and engineering of data transport technologies used in network centric warfare and how changes in components and data priorities affect the overall performance of the data transport system for an organization. Conversely, there is also a need to achieve a better understanding of how data should be prioritized in order to best meet each user's needs in conjunction with the overall organization's needs. In future work, we intend to explore both of these avenues of research based upon the formulation for data transmission presented in this paper.

References

[1] Alberts, D.S.; Garstka, J.J.; Hayes, R.E.; and Signori, D.T. (2001) *Understanding Information Age Warfare*. CCRP Press, CCRP Publication Series: Washington D.C.

[2] Alberts, D.S. and Papp, D.S. (2001) *Information Age Anthology, Volumn 1: The Nature of the Information Age*. CCRP Press, CCRP Publication Series: Washington D.C.

[3] Alberts, D.S.; Garstka, J.J.; and Stein, F.P. (1999) *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Press, CCRP Publication Series: Washington D.C.

[4] Alberts, D.S. (2002) *Information Age Transformation: Getting to a 21st Century Military*.

CCRP Press, CCRP Publication Series: Washington D.C.
[5] Alberts, D.S. and Hayes, R.E. (2003) *Power to the Edge* CCRP Press, CCRP Publication Series: Washington D.C.
[6] Command and Control Research Program (2002) *The Code of Best Practices for Experimentation*. CCRP Press, CCRP Publication Series: Washington D.C.
[7] Garstka, J.J. (2000) "Network Centric Warfare: An Overview of Emerging Theory," *PHALANX*, Military Operations Research Society, Alexandria, VA.
[8] Miller, G.A. (1956) "The Magical Number Seven Plus or Minus Two: Some Limits on Our Capacity for Processing Information," *The Psychology Review*, vol. 63.
[9] NATO SAS026 (2003) *Nato Code of Best Practice for C2 Assessment*. CCRP Press, CCRP Publication Series: Washington D.C.
[10] Smith, E.A. (2003) *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*. CCRP Press, CCRP Publication Series: Washington D.C.

NETWORK AND DATA POLICY CONSIDERATIONS FOR EFFECTIVE NETWORK CENTRIC OPERATIONS

J. Katharine Burton
Institute for Defense Analyses
Washington, DC
kburton@ida.org

Martin R. Stytz, Ph.D.
Institute for Defense Analyses
Washington, DC
mstytz@ida.org ,mstytz@att.net

Gregory N. Larsen, Ph.D.
Institute for Defense Analyses
Washington, DC
glarsen@ida.org

Introduction

- Change to network centric operations (NCO) is placing unprecedented demands upon the US military and its capability to rapidly adopt new technologies
  - NCO places a premium on information timeliness
  - Information as force multiplier
- Technology, policy, and doctrine under development
- However, lacking in ability to effectively knit advances together to maximize effectiveness
  - Unclear how to translate policy into resource allocations
    - Network resources
    - Data

Need an overall systems engineering approach, point solutions are <u>not</u> likely to be scalable or sufficient

Introduction (cont.)

- We examine network and data policies and issues to achieve effective NCO
  - Technologies and policies
- Network and data control and management policy are critical
  - Address NCO needs
  - Manage and make effective use of network and control information flow
- Policies should be driven by needs and capabilities of users of NCO data
  - Also consider bandwidth, communication alternatives, priorities, and data security
- Changes in policy must be made rapidly
  - Placing a premium on cyber situation awareness and tools for translating decisions into policy
- But, lack metrics

Factors to Consider

- Mission for each organization
- Battlespace state
- Available communication channels
- User and commander data needs
- User and commander security demands
- These factors define the required veracity, timeliness, truthfulness and data verification requirements
- Need for speed and complexity point to need for intelligent agent assistance and tools

Network and Data Policy Requirements

- **Capabilityof a NCO force correlates with ability of data to move to where it is needed**
  - **Effectively & efficiently**
- **Need to understand data volume requirement imposed**
  - **Let $I_{r_a} \leftarrow I_{s_b}$ be the instantaneous data volume between any source and recipient**
  - **Then, total data volume need for an organization is defined as:**
    - **$I_1 = \left(\prod_{i=1}^{n} I_{r_i} \leftarrow \prod_{j=1}^{m} I_{s_j} \right)$**
    - **An effective NC organization must have as large an I_1 as possible**

Data Velocity and Data Traversal

- ω
- At a given time, T, the data velocity is defined as:
  - $(I_{1\tau} - I_{1\tau-1}) / I_{1\tau-1}$
- Data traversal is defined as I_2, which is
  - $I_2 = \left(\left(\prod_{i=1}^{n} I_{r_i} \leftarrow \prod_{j=1}^{m} I_{s_j}\right)\right) \div \sum\left(\Delta t(r_i \leftarrow s_j) \ \forall \ (r_i \leftarrow s_j) \neq 0\right)$
- I_2 must be minimized
  - No contention for bandwidth
  - Data moves promptly
- Must consider time required for priority data to arrive at its destination
  - Call this priority data *y*

Priority Data Considerations

- I_{3p} is the average time for priority data to move all sources to all recipients of data of a given priority, *p*
  - P_y is the set of priority data of a given priority in movement at any time
  - P_y, y=1,x is the set of all priorities for data
  - I_{3p} at time y is defined as:

$$\left(\left(\prod_{i=1}^{n} I_{r_i} \leftarrow \prod_{j=1}^{m} I_{s_j}\right)\right) \div \sum\left(\Delta t\left(r_i \leftarrow s_j\right)\left[\ni\left(\left(r_i \leftarrow s_i\right) \neq 0 \wedge \left(r_i \leftarrow s_j\right) \subset p_y\right)\right]\right)$$

  - Allowing I_3 to be defined as

$$\sum_{y=1}^{x} I_{3_{p_y}} \div x$$

Need Differential

- I_4 is defined as the difference between when the data is needed and when it arrives at a recipient
  - For a given time period
  - Must be minimized for each recipient and the organization
- I_4 for a recipient *r* is defined as:

$$\sum_{j=1}^{m}\left(ta_r - tn_r\right) \forall \left(I_r \leftarrow \prod_{j=1}^{m} I_{sj} \ni \left(r_r \leftarrow s_j\right) \neq 0\right)$$

- For the organization, I_4 can then be defined as:

$$\sum_{r=1}^{n} \mathrm{I}_{4_r}$$

- I_3 for a recipient must be minimized in order to minimize I_4

Need Differential for Data of a Priority

- I_5 is defined as the time differential between when the dat of a given priority is needed by a recipient and when it arrives
- I_5 for a recipient is then defined as follows:

$$\sum_{j=1}^{m}\left(ta_r - tn_r\right) \forall\ I_r \leftarrow \prod_{j=1}^{m} I_{s_j}\ \ni \left(\left(\left(r_r \leftarrow s_j\right) \neq 0\right) \wedge \left(\left(r_i \leftarrow s_j\right) \subset p_y\right)\right)$$

- Should approach zero for data of highest priority for each data recipient

Data Movement Efficiency

- Ψ
- Defined for each recipient at a given time
- Data efficiency is based on performance as measured by I_4
- Ψ for a given recipient for a given time is defined as:
  - $\psi_{r\tau} = (I_{4r\tau} - I_{4r\tau-1}) / I_{4r\tau-1}$

Further Considerations on Data Transport

- Data transport time, I_2, is based upon
  - Time spent in transit in a medium
  - Time spent in computing devices
  - Time spent in sensor systems
  - Time spent in releasibility decision making
  - Time spent in analysis
- Transit, computing, and sensor times are nearly constant
- Key is minimizing releasibility and analysis time
  - Argues for automation of these critical but sensitive tasks
    - Intelligent agents
      - For prioritization as well as information overload management
  - Same conclusions appear to hold for I_3, I_4, I_5

Need an overall systems engineering approach, point solutions are <u>not</u> likely to be scalable or sufficient

Major Metrics Redux

Metric/ Variable	Definition
I_1	The volume of data moving from all sources of data to all recipients of data within an organization at any given time
I_2	The average time for data to move from all sources to all recipients within a time period
I_3	The average elapsed time for priority data of a given priority to move from all sources to all recipients of data of that priority at any given time.
I_4	The time differential between the time when data is needed by a recipient and when it is received.
I_5	The time differential between the time when data is needed by a recipient and when it received by the data recipient for a given time period for data of a given priority.
$\varpi\ \tau$	Data velocity within an organization at a time τ
ψ	The efficiency of the movement of data.

Policy Implications

- Lacking tools and instrumentation to make required measurements in real time
- Lack insight into details, components, and placement of the metrics
- Must be able to deal with rapid changes in data transport requirements
- Intelligent agents are critical
- Technology preparedness is crucial
  - No alternative but to be at cutting edge of communication and computing technologies
  - Tools
- Simulation to gain understanding of metrics and their components is critical
  - No one solution for all situations, further complicating the challenge
  - Tools

Conclusions and Future Work

- NCO places a premium on network and computing technologies and policies
- We presented metrics to assess effectiveness of technologies and policies
- Need more detailed representations of the metrics
  - Experimentation and theoretical
  - Topologies, bandwidth, cyberwarfare, coalition, other factors
- Susceptibility to cyberoperations will determine effectiveness of a NCO force
- Coalition complicates NCO challenges
  - The metrics we propose can be used to assess effectiveness of coalition communication

Future Work

- Extend metrics proposed here
  - Develop component representations
- Need real-time network instrumentation to enable management of network
  - Sensors, data needed, dissemination
- Need training to prepare for cyberattacks
- Need insight into systems engineering for NCO networks
  - Better end-to-end engineering to insure efficient, prioritized data transport
- Better insight into user needs for data
  - Proper prioritization